Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers	)	WC Docket No. 16-106
of Broadband and Other	)	
Telecommunications Services	)	

COMMENTS OF ZEOTAP GMBH

zeotap GmbH ("zeotap") submits these comments in support of petitioners that ask the Federal Communications Commission ("FCC" or "Commission") to reconsider the rules governing broadband Internet access service ("BIAS") providers that were adopted in the *2016 BIAS Privacy Report and Order*.[1] As discussed below, those rules: (i) contravene Section 222 of the Communications Act; (ii) rely on inaccurate assumptions about the mobile advertising industry; (iii) improperly impose one-size-fits-all rules on de-identified data without weighing the costs and benefits of doing so; and (iv) unnecessarily depart from the Federal Trade Commission's ("FTC") longstanding data privacy and security enforcement framework.

A leader in the mobile advertising industry, zeotap partners with BIAS providers and other companies to serve consumers highly relevant, useful mobile advertisements. At the core of zeotap's platform is a cutting-edge proprietary technology to de-identify data. Notwithstanding this robust privacy-by-design architecture, the FCC's rules could unnecessarily impede services offered by zeotap and other mobile advertising platforms. This illogical outcome is the product of the Commission's categorical treatment of BIAS providers' data use

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, 31 FCC Rcd 13911, FCC 16-148, WC Docket No. 16-106 (rel. Nov. 2, 2016) ("*2016 BIAS Privacy Report and Order*").

and sharing practices for non-aggregate data, regardless of whether such data has been de-identified.

The record, however, shows that the Commission's categorical treatment of de-identified data is without basis. The reality is that BIAS providers can provide "ad targeting both in their own businesses and in partnership with third party ad networks"—such as zeotap—that "use de-identified data to enable privacy protective advertising that poses minimal risk to consumers and is typically subject to opt out controls."[2] Where strong de-identification safeguards foreclose any reasonable risk of identifying a specific named individual, the Commission's rules fail even a basic cost-benefit analysis: they do nothing to provide additional safeguards for end-users' privacy interests while frustrating innovative business models, thwarting competition for new ad-supported services, and potentially increasing the cost of Internet content for consumers.

I. ZEOTAP'S MOBILE ADVERTISING PLATFORM DELIVERS HIGHLY RELEVANT CONTENT TO CONSUMERS WHILE HELPING TO PROTECT THEIR INDIVIDUAL PRIVACY.

There has been a proliferation of technologies that enable targeted ads on the Internet. The economic reasons for this growth are well-known and amply documented in the record before the FCC.[3] Consumers may be unwilling to pay directly for content and apps that they nevertheless find interesting and useful, and this content must therefore be ad-supported to be economically viable. Some websites and apps, however, have difficulty supporting their businesses with advertising. Ad impressions are frequently sold very cheaply because they are poorly placed, although advertisers are willing to pay more for ads tailored to consumers'

[2] Reply Comments from Future of Privacy Forum, WC Docket No. 16-106, at 4 (July 6, 2016) ("FPF Reply Comments").
[3] *See, e.g.*, *Comments of Maureen Ohlhausen of the Federal Trade Commission*, WC Docket No. 16-106 (May 27, 2016) (suggesting that "ad-supported broadband services" can "increase broadband adoption").

interests. As Chairman Pai has recognized, the value of Internet advertising critically supports the viability of free content—a key engine of Internet and mobile application growth.[4]

zeotap's proprietary mobile advertising platform combines different layers of data to serve relevant ads. Because it sits squarely in the middle of the mobile advertising ecosystem, zeotap's platform helps to bring together BIAS providers, advertisers, publishers, and their respective ad networks. A startup founded in 2014, zeotap has raised more than $20 million in funding[5] and has become a global leader that partners with BIAS providers and other large companies outside the communications industry.

zeotap's platform also represents a market-driven solution to the growing consumer demand for privacy, incorporating privacy-by-design safeguards into its targeting algorithms. The information that zeotap receives from BIAS providers is mapped to an advertising identifier ("AD ID") generated by the operating system of the device. AD IDs are commonly used in the online advertising ecosystem to facilitate the sale and placement of targeted advertising and are associated with a device, not an individual. Unlike other ad services providers, however, zeotap does not share AD IDs with or make them available to third parties; rather, zeotap uses randomly generated brand-new, temporary identifiers that cannot be used to trace back to the individual who owns the device.

zeotap implements numerous safeguards in connection with the provision of these identifiers to help minimize the risk of data leakage or re-identification. No personally identifiable or traditionally sensitive data is associated with the identifier. To the extent that

---

[4] *Examining the Proposed FCC Privacy Rules*, Hearing Before the S. Comm. on the Judiciary, Subcomm. on Privacy, Tech., and the Law, 114th Cong. (2016), Testimony of Commissioner Ajit Pai, at 1, 3, http://bit.ly/24W3FiY.

[5] Anthony Ha, *Mobile data startup Zeotap raises €12M*, TechCrunch (Jan. 12, 2017), http://tcrn.ch/2j6YXwu; Christina Kyriasoglou, *Hitfox-Startup Zeotap bekommt sechs Millionen Euro*, Gründerszene (Aug. 4, 2015), http://bit.ly/2mlmCOm.

demographic information is tied to the identifier, zeotap ensures that these categories are sufficiently broadly defined (*e.g.*, "car enthusiasts") to prevent the possibility of re-identification. zeotap does not act as a data broker. Its clients, partners, and third parties do not have access to the underlying ISP customer data.

zeotap's platform is also consistent with the goal of promoting consumer choice. Users can opt out of sharing through BIAS providers' existing opt-outs mechanisms, whether based on the carrier's subscriber ID or the web-based AD ID opt-out that zeotap may make available on behalf of carriers. Moreover, consumers can prevent zeotap's use of non-identifiable demographic information collected for targeted advertising by changing the setting on their mobile device to "Limit Ad Tracking." Finally, consumers can reset the advertising identifier on their device, which would eliminate any device profile and result in a newly generated AD ID.

II. THE COMMISSION SHOULD REVISE ITS BIAS PRIVACY AND SECURITY RULES.

A. The FCC's Categorical Treatment of Non-Aggregate Data, Regardless of the Level of De-Identification, Contravenes Section 222 of the Communications Act and Hinders Privacy-Protective Services Like zeotap that Promote Competition and Reduce Costs.

The Commission's failure to perform a cost-benefit analysis of the BIAS privacy and security rules is itself more than enough to merit reconsideration. This methodological flaw has produced an overbroad definition of de-identified data, which excludes any data reasonably linkable to a *device*, regardless of whether it can ever be used to identify an *individual*.[6] As Chairman Pai noted, this definition is based on an unwarranted assumption that device identifiers are always *persistent* in nature.[7] That assumption is false. Conspicuously absent from the Commission's analysis is a reasoned discussion of randomly generated, temporary identifiers

[6] *See 2016 BIAS Privacy Report and Order* ¶ 114.
[7] *Id.* at Dissenting Statement of Commissioner Ajit Pai; *id.* at n.311 (citing to examples relating to persistent device identifiers).

that are frequently reset. The Commission's omission of the possibility "that persistent online identifiers (like static IP addresses) pose a larger privacy issue than more transitive identifiers"[8] represents a failure to conduct a rigorous analysis. For example, a framework that allows for transitive identifiers would encourage the use of "privacy-protective technologies."[9]

The Commission erroneously states that this categorical treatment is appropriate because device identifiers are increasingly becoming proxies to identify individuals.[10] Regardless of whether that is sometimes or even frequently true, it is not always so—nor does the Commission even claim that it is. As the Future of Privacy Forum correctly observes, skepticism over whether certain data can ever be fully de-identified "misses the point that de-identification is not a one-size-fits-all approach."[11] Where it is logically impossible for a device identifier to connect to an individual, the consumer privacy benefits of additional heavy-handed regulation are non-existent. That point is particularly salient here, where companies like zeotap act as privacy-protective barriers keeping end-users (*i.e.*, advertisers) from the data inputs provided by the underlying source (*i.e.*, ISPs and their customers).

Moreover, the Commission's rules improperly fixate on whether the BIAS provider is the entity that de-identifies its data. In doing so, it fails to consider situations where BIAS providers share personally identifiable information ("PII") that is immediately de-identified and then siloed or purged, ultimately providing significant protection against misuse. By preventing third parties from doing that which BIAS providers could permissibly themselves do, the BIAS Privacy Rules impose unnecessary costs on a variety of consumer-enhancing practices and foreclose specialization among firms.

[8] *Id.* at Dissenting Statement of Commissioner Ajit Pai.
[9] *Id.*
[10] *See, e.g., id.* at n.168.
[11] FPF Reply Comments at 3.

As Commissioner O'Rielly has recognized, a properly conducted cost-benefit analysis would have revealed that "consumer privacy has been adequately protected under the current FTC framework and that there has been no evidence of any privacy harms."[12] At the same time, as he noted, the new rules will result in "increased transaction costs to purchase the information," as well as "the foreclosure of innovative services that providers won't be able to offer and consumers won't receive."[13] These costs "will ultimately be passed on to consumers."[14]

Not only is the Commission's treatment of de-identified data unsound from a cost-benefit standpoint, it is unmoored from Section 222 of the Communications Act governing customer proprietary network information ("CPNI"). Section 222 provides that "individually identifiable" CPNI may not be used, disclosed, or permitted access without customer consent or unless otherwise authorized by law.[15] The Commission's rules fail to give effect to Congress's use of the phrase "individually identifiable," which does not encompass *device identifiers* that do not identify an individual person. No colorable interpretation of Section 222 permits the Commission to treat CPNI purged of personal identifiers as "individually identifiable." Yet that is precisely what the Commission's privacy rules do here.

The Commission's unlawful rules governing de-identified data will inflict real harm to the mobile advertising industry and companies, like zeotap, that build privacy into the core of their platforms. There is no good reason to restrict sharing and use practices where third parties de-identify BIAS data and eliminate any reasonable possibility of individual re-identification.

[12] *2016 BIAS Privacy Report and Order* at Commissioner O'Rielly dissent; *see also id.* at Commissioner Pai dissent.
[13] *Id.* at Commissioner O'Rielly dissent.
[14] *Id.*
[15] 47 U.S.C. § 222(c)(1).

B. The Commission Should Harmonize Further the BIAS Rules with the FTC's Time-Tested Data Privacy and Security Framework.

As Chairman Pai and Commissioner O'Rielly have noted, the FCC has unreasonably adopted BIAS privacy rules that represent a "significant departure from the FTC approach, which is the basis for current expectations."[16] In particular, by classifying web browsing history and app usage as categorically "sensitive" information and requiring heightened notice and opt-out treatment, the Commission has significantly departed from well-settled U.S. data privacy and security principles.

Categorically treating such information as sensitive assumes that its collection and use inherently carries a risk of consumer injury. It does not. Knowledge that a consumer has visited a weather forecast website, for instance, bears no necessary (or even likely) relationship to the harms traditionally associated with data misuse—identity theft, financial loss, or harassment. No credible evidence on the record supports lumping together all browsing history and app usage information as a singular category justifying heightened scrutiny across-the-board. And there is simply no robust data in the record to suggest that ISPs' collection and use of this data chill consumer behavior or degrade the quality of service. To the contrary, data speeds are increasing, and U.S. Internet usage continues to grow at a rapid pace.[17]

The FTC has carefully considered these issues, and it has concluded that reasonable consumer expectations and the realistic likelihood of injury do not justify categorically heightened protection of browsing and app information. While the FTC has recognized the sensitivity of "data about children, financial and health information, Social Security numbers, and certain geolocation data," it has not deemed browsing and app usage history to be

[16] *Id.* at Dissenting Statement of Commissioner O'Rielly.
[17] *See generally* Cisco, *The Zettabyte Era: Trends and Analysis* 2 (Jun. 2, 2016) ("Broadband speeds will nearly double by 2020. By 2020, global fixed broadband speeds will reach 47.7 Mbps, up from 24.7 Mbps in 2015."), *available at* http://bit.ly/2aeYBCg.

categorically "sensitive."[18] For that reason, "online retailers and services such as Amazon.com and Netflix need not provide choice when making product recommendations based on prior purchases."[19]

The FTC's approach makes sense. Browsing history and app usage information are qualitatively different from the other data elements the FCC has categorized as "sensitive"—social security numbers, financial information, health information, and children's information, among others. There are at least three differences.

First, the release of traditionally "sensitive" data carries an inherent and concrete risk of harm. For example, the unauthorized disclosure of social security numbers directly relates to identity theft, and the release of payment card information poses a significant risk of financial loss. By contrast, the harm associated with the release of browsing history and app usage data is *speculative*. To be sure, harm could theoretically materialize, but only if a number of contextual assumptions hold. That presents a poor case for the type of stringent, *ex ante* regulatory treatment adopted here.

Second, information traditionally considered "sensitive" enters the stream of commerce through identifiable and limited channels.[20] Health, financial, and social security information are obtained through specific conduits—frequently involving a special relationship, such a medical provider or a bank—and are customarily encrypted in online transactions. None of these features exist with respect to browsing and app usage history, which are content- and relationship- neutral categories that are accessed by multiple channels in every web transaction (*i.e.*, the device, operating system, browser or application, edge service provider, and ISP).

---

[18] *See* Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers* 47 (2012) ("FTC Report").
[19] FTC Report at 48.
[20] *See Ex Parte* Letter from Scott K. Bergmann, Vice President of Regulatory Affairs, CTIA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 6 (Sept. 16, 2016).

Third, federal statutory protections frequently accompany traditionally "sensitive" data categories—*e.g.*, Health Insurance Portability and Accountability Act (health), Gramm-Leach-Bliley Act (financial), Privacy Act (social security), Children's Online Privacy Protection Act (children). These laws provide extrinsic congressional evidence in support of data's sensitivity. No similar statutory regime supports the sensitivity of browsing and app usage information. To the contrary, by adopting the narrow CPNI requirements, Congress expressly limited the category of uniquely sensitive information arising from the relationship between BIAS providers and their consumers. As others have persuasively demonstrated, Section 222, which is limited to CPNI, does not provide a statutory *carte blanche* to regulate a "new, made-up category of information that the Commission calls 'customer proprietary information'" that includes web-browsing and app usage history.[21]

* * *

For the foregoing reasons, the Commission should grant the petitions for reconsideration and rescind or modify the BIAS privacy and security rules, especially those governing de-identification.

Respectfully submitted,

/s/ Daniel Heer

Daniel Heer, Managing Director
zeotap GmbH
Poststraße 12, 10178
Berlin, Germany
Telephone: +49 30 55578678
Daniel.Heer@zeotap.com

zeotap

March 6, 2017

[21] *See* Petition for Reconsideration of CTIA, WC Docket No. 16-106, at 3 (Jan. 3, 2017).